



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant : Kravitz
Serial No. : 10/010995 Examiner: To be assigned
Filed : October 19, 2001 Group Art Unit: To be assigned
For : CRYPTOGRAPHIC DATA SECURITY SYSTEM AND
METHOD

INFORMATION DISCLOSURE STATEMENT

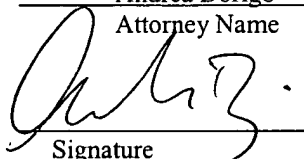
I hereby certify that this paper is being deposited with the United States Postal Service as first class mail in an envelope addressed to:
Assistant Commissioner for Patents, Washington, D.C. 20231

January 22, 2002

Date of Deposit

Andrea Dorigo

Attorney Name



Signature

47,532

PTO Registration No.

January 22, 2002

Date of Signature

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

Applicants, by their attorneys, hereby bring the following documents to the attention of the Examiner in connection with the examination of the above-captioned patent application:

Juels, A., et al., "*Client Puzzles: a Cryptographic Countermeasure Against Connection Depletion Attacks*," February 4-5, 1999, Network and Distributed System Security Conference, San Diego, California; revised version published on-line at <http://www.rsasecurity.com/rsalabs/staff/bios/ajuels>.

"Securing your Future with Two-factor Authentication," published on-line at <http://www.rsasecurity.com/products/secuid/index.html>

R. Rivest, A. Shamir, and L. Adleman, "*A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*," Communications of the Association for Computing Machinery, Vol. 21, pp. 120-26 (February 1978).

M. Bellare and P. Rogaway, "*Optimal Asymmetric Encryption*," Advances in Cryptology – Eurocrypt '94 (May 9-12, 1994), published in Lectures in Computer Science, A. DeSantis Ed., Springer Verlag, vol. 950, pp. 92-111 (1995).

M. Bellare and P. Rogaway, "*Optimal Asymmetric Encryption – How to Encrypt with RSA*", revised version of Optimal Asymmetric Encryption paper: published on-line at <http://www-cse.ucsd.edu/users/mihir/papers/oaep.html> ((November 19, 1995).

D. B. Johnson and S. M. Matyas, "*Asymmetric Encryption: Evolution and Enhancements*," Cryptobytes, Volume 2, No. 1 (Spring 1996)

"*Data Encryption Standard (DES)*," October 25, 1999, published on-line at <http://csrc.nist.gov/cryptval/des.htm>, link FIPS 46-3.

"*DES Modes of Operation*," December 2, 1980, published on-line at <http://csrc.nist.gov/cryptval/des.htm>, link FIPS 81.

K. M. Martin, B. Preneel, C. J. Mitchell, H. J. Hitz, G. Horn, A. Poliakova, and P. Howard, "*Secure Billing for Mobile Information Services in UMTS*," Proceedings of Intelligence and Services in Networks, Antwerp, Belgium (May 25-28, 1998).

M. O. Rabin, "*Digitalized Signatures and Public-key Functions as Intractable as Factorization*," Massachusetts Institute of Technology Laboratory for Computer Science Technical Report 212 (1979).

S. W. Smith, "*Secure coprocessing applications and research issues*," Los Alamos Unclassified Release LA-UR-96-2805 (August 1996).

U. G. Wilhelm, S. Staamann, and L. Buttyan, "*On the Problem of Trust in Mobile Agent Systems*," Proceedings of Network and Distributed Systems Security, San Diego, California (March 11-13, 1998).

B. Yee, "*Using Secure Coprocessors*," Carnegie Mellon University Report CMU-CS-94-149 (May 1994).

R. Mori and M. Kawahara, *"Superdistribution: the Concept and the Architecture,"* The Transactions of the IEICE, vol. E73, no. 7, Special Issue on Cryptography and Information Security (July 1990). Full on-line text published on-line at: <http://www.virtualschool.edu/mon/ElectronicProperty/MoriSuperdist.html>.

M. Blum, W. Evans, P. Gemmell, S. Kannan, and M. Naor, *"Checking the Correctness of Memories,"* Algorithmica, 12(2/3), pp. 225-244 (1994).

B. Askwith, M. Merabti, Q. Shi and K. Whiteley, *"Achieving User Privacy in Mobile Networks,"* Proceedings of the 13th Annual Computer Security Applications Conference, San Diego, California (December 8-12, 1997). Full text available to Insitute of Electrical and Electronic Engineers, Inc. Computer Society members with web account, or to others through purchase of individual article, at: <http://china.computer.org/proceedings/acsac/8274/8274toc.htm>.

C. H. Lim and P. J. Lee, *"A Key Recovery Attack on Discrete Log-based Schemes Using a Prime Order Subgroup,"* August 17-21, 1997, Advances in Cryptology: Crypto '97, Santa Barbara, California, B.S. Kaliski, Jr., Ed., Lecture Notes in Computer Science 1294, pp. 249-263, Springer-Verlag.

J. Horn and B. Preneel, *"Authentication and Payment in Future Mobile Systems,"* Proceedings of European Symposium On Research In Computer Security, Louvain-La-Neuve, Belgium (September 16-18, 1998).

D. Chaum and T. P. Pedersen, *"Wallet Databases with Observers,"* August 16-20, 1992, Advances in Cryptology: Crypto '92, Santa Barbara, California, E.F. Brickell, Ed., Lecture Notes in Computer Science 740, pp. 89-105, Springer-Verlag.

"The Digital Dilemma: Intellectual Property in the Information Age," Committee on Intellectual Property Rights in the Emerging Information Infrastructure, Washington, D.C., National Academy Press, 2000. Full on-line text published at http://books.nap.edu/html/digital_dilemma.

B. Patel and J. Crowcroft, *"Ticket based service access for the mobile user,"* Proceedings of Mobicom '97, Budapest, Hungary (1997). Full text available through ACM Digital Library Document Delivery Service at <http://portal.acm.org/citation.cfm?id=262116.262150&coll=ACM&dl=ACM&type=series&idx=SERIES395&part=series&WantType=Proceedings&title=International%20Conference%20on%20Mobile%20Computing%20and%20Networking&CFID=915821&CFTOKEN=26102377#>

M. Stefik, *"Trusted systems,"* Scientific American, pp. 78-81 (March 1997). Published on-line at <http://www.sciam.com/0397issue/0397stefik.html>.

B. Kaliski, *"New Challenges in Embedded Security,"* Consortium for Efficient Embedded Security Symposium on Embedded Security, Security Ownership and Trust Models (July 10, 2001). Published on-line at <http://www.cesstandards.org>.

J. Manferdelli, *"digital Rights Management,"* Consortium for Efficient Embedded Security Symposium on Embedded Security, Security Ownership and Trust Models (July 10, 2001). Published on-line at <http://www.cesstandards.org>.

M. Rotenberg, *"Consumer Implications of Security Applications,"* Consortium for Efficient Embedded Security Symposium on Embedded Security, Security Ownership and Trust Models (July 10, 2001). Published on-line at <http://www.cesstandards.org>.

S. Pugh, *"The Need for Embedded Security,"* Consortium for Efficient Embedded Security Symposium on Embedded Security, Security Ownership and Trust Models (July 10, 2001). Published on-line at <http://www.cesstandards.org>.

L. Buttyan and J.-P. Hubaux, *"Accountable Anonymous Access to Services in Mobile Communications Systems,"* 1999, Proceedings of the 18th Institute of Electrical and Electronic Engineers Symposium on Reliable Distributed Systems (SRDS).

"RSA SecurID Authentication - A Better Value for a Better ROI," published on-line at <http://www.rsasecurity.com/products/securid/index.html>.

A PTO-1449 form and a copy of each of the above-listed documents is enclosed.

The Commissioner is hereby authorized to charge payment of any fees associated with this communication or credit any overpayment to Deposit Account No. 02-4377.

Respectfully submitted,

A handwritten signature in cursive script, appearing to read 'Andrea Dorigo', is written over a horizontal line.

Andrea Dorigo
Patent Office Reg. No. 47,532

Agent for Applicants
(212) 408-2523

Enclosures